UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/870,584	06/01/2001	Frank W. Sudia	P 264493 AUTH-II	9326

909 7590 07/15/2008

PILLSBURY WINTHROP SHAW PITTMAN, LLP
P.O. BOX 10500
MCLEAN, VA 22102

EXAMINER	
DADA, BEEMNET W	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
07/15/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/870,584	SUDIA ET AL.	
	Examiner	Art Unit	
	BEEMNET W. DADA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 April 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,18-21,72-84 and 109-131* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,18-21,72-84 and 109-131* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 June 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. In view of the Appeal Brief/Pre-Appeal brief Conference request filed on 04/08/2008, PROSECUTION IS HEREBY REOPENED. New grounds of rejection are set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR **1.111** (if this Office action is non-final) or a reply under 37 CFR **1.113** (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR **41.31 followed by an appeal brief under 37 CFR 41.37**. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in **37 CFR 41.20** have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

Priority

2. This application is a continuation of application No. 08/786,046, filed on 01/21/1997. Therefore, the effective filling data for the subject matter defined in the pending claims of this application is January 21, 1997.

3. Claims 2-17, 22-71 and 85-108 are canceled. Thus **1, 18-21, 72-84 and 109-131** are pending/examined, of which claims **1, 73 and 79** are independent claims.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. **Claims 1, 18-21, 72-84 and 109-131** are rejected under 35 U.S.C. 102(b) as being anticipated by SUDIA, Frank, W. (hereinafter Sudia) (European Publication No. EP 0771499B1, (Date of publication and mention of the grant of the Patent (**09/28/2005**) (See attached).

6. **As per independent claim 1, Sudia discloses in a cryptographic system** *[See figure 14 and paragraph 0084, "cryptographic system"]* **wherein a certifying authority issues digital certificates identifying users of said system,** *[paragraph 0085, figure 14, ref. Num "1404"] (on paragraph 0085, referring to figure 14, the following has been disclosed. "a certifying authority CA 1402 issues user identity certificate 1404 to users")* **said digital certificates being digitally signed with a private key of said certifying authority to form a digital signature [Paragraph 0085, figure 14, ref. Num "1410"]** *(On paragraph 0085, the following has been disclosed. "Certifying authority 1402 has a private key 1406 and a public key 1408. The private key 1406 is used to digitally sign the certificates 1404 with certifying authorities digital signatures 1401]* **and requiring a public key of said certifying authority in order to verify said digital signature, [paragraph 0086, last sentence]** *(On paragraph 0086, last sentence the following has been disclosed. "in order for the information contained in the certificates 1404 to be verified by other users of the system, these other users must have access to the public key 1408 of the certifying authority 1402)* **and wherein a user transaction in said cryptographic system requires verification by a recipient of said**

user transaction, said verification based on information in said digital certificates and requiring said public key,[See paragraph 0086, last sentence, paragraph 0087 and paragraph 0091] *(On paragraph 0091, the following has been disclosed. "As noted above in order for the information contained in the various certificates to be verified by users of the system, these users must have access to the public key 1408 of the certifying authority 1402")* **a method of controlling use of said public key** *[paragraph 0091-0092],(On paragraph 0091, the following has been disclosed. "In order to enforce the rules of each certifying authority in the system it is necessary to limit the access to the public key 1408 of some of the certifying authorities. In particular it is necessary to limit access to the public key of the topmost (root) certifying authority 1402")* **comprising:**

- **providing said recipient with at least one message containing rules of said system, said rules including a rule regarding maintaining secrecy of said public key** *[Paragraph 0092, lines 13-18] (On paragraph 0092, the following has been disclosed. "Accordingly, the root certifying authority 1402 keeps its public key a trade secret, and in order to obtain the public key of the root certifying authority 1402, a user (potential recipient) 1424 wishing to undertake transactions in the system must obtain the certifying transactions rules 1426 issued by the root certifying authority.)*

- **by said recipient, digitally signing said at least one message, by which said recipient agrees to said rules; [***Paragraph 0092, lines 18-22] (On paragraph 0092, lines 18-22, the following has been disclosed. "Recipient 1424 must hash these rules to form hashed rules 1428 which it must then digitally sign to produce a signed copy of the hashed rules 1430, This digitally signed copy of the hashed rules must be returned to the root certifying authority 1402")* **and**

- **In response to said digital signing, permitting said recipient to utilize said public key and prior to said digital signing, denying utilization of said public key.[paragraph 0093]** *(On paragraph 0093, the following has been disclosed. "Once the root certifying authority 1402 is satisfied that it has received a valid copy of the system rules signed by the recipient 1424, the root certifying authority issues its public key 1408 to the recipient 1424")*

7. **As per independent claim 73, Sudia discloses a method of enforcing a security policy in a cryptographic system, said policy including controlling use of a public key utilizable by a plurality of users of the cryptographic system,** *[paragraph 0091-0092],(On paragraph 0091, the following has been disclosed. "In order to enforce the rules of each certifying authority in the system it is necessary to limit the access to the public key 1408 of some of the certifying authorities. In particular it is necessary to limit access to the public key of the topmost (root) certifying authority 1402")* **said method comprising:**

- **providing a recipient with a message containing rules of said cryptographic system, said rules including a rule regarding maintaining secrecy of said public key***[Paragraph 0092, lines 13-18] (On paragraph 0092, the following has been disclosed. "Accordingly, the root certifying authority 1402 keeps its public key a trade secret, and in order to obtain the public key of the root certifying authority 1402, a user (potential recipient) 1424 wishing to undertake transactions in the system must obtain the certifying transactions rules 1426 issued by the root certifying authority.)*

; and

- **in response to said recipient digitally signing said message, by which said recipient agrees to said rules, [***Paragraph 0092, lines 18-22] (On paragraph 0092, lines 18-22, the following has been disclosed. "Recipient 1424 must hash these rules to form hashed*

rules 1428 which it must then digitally sign to produce a signed copy of the hashed rules 1430, This digitally signed copy of the hashed rules must be returned to the root certifying authority 1402") **permitting said recipient to utilize said public key and prior to said recipient digitally signing said message, denying use of said public key [paragraph 0093]** *(On paragraph 0093, the following has been disclosed. "Once the root certifying authority 1402 is satisfied that it has received a valid copy of the system rules signed by the recipient 1424, the root certifying authority issues its public key 1408 to the recipient 1424")*

8. **As per independent claim 79, Sudia discloses a method of enforcing a security policy in a cryptographic system, said policy including controlling use of a public key,** *[paragraph 0091-0092],(On paragraph 0091, the following has been disclosed. "In order to enforce the rules of each certifying authority in the system it is necessary to limit the access to the public key 1408 of some of the certifying authorities. In particular it is necessary to limit access to the public key of the topmost (root) certifying authority 1402")* **said method comprising:**

- **providing a recipient with a message containing rules of said system and with a secure device containing an inactive form of said public key, wherein said public key cannot be obtained from said device***[paragraph 0094, figure 14, ref. Num "1436"] (On paragraph 0094, the following has been disclosed. "the root certifying authority public key 1424 may be issued to a recipient in a number of ways. In preferred embodiments the recipient is provided with a secure device 1436". Furthermore on the same paragraph the following has been disclosed. "the certifying authority public key 1408 is in the device 1436 in a disabled form..."];* **and**

- **in response to said recipient digitally signing said message, activating said public key in said secure device.***[Paragraph 0094, last sentence] (On paragraph 0094, last sentence the following has been disclosed, "in another preferred embodiment, the certifying*

authority public key 1408 is in the device 1436 in a disabled form, and the root certifying authority 1402 enables the key 1408 in the device upon receipt and verification of the signed rules 1430")

9. **As per dependent claims 18, 74, 119, 122-124 and 127 Sudia** discloses a method of enforcing a security policy in a cryptographic system, said policy including controlling use of a public key as applied to claims above. **Furthermore Sudia** discloses a method wherein said providing includes providing said recipient with a secure device containing said public key, wherein said public key cannot be obtained from said secure device. *[Paragraph 0094, last sentence] (On paragraph 0094, last sentence the following has been disclosed, "in another preferred embodiment, the certifying authority public key 1408 is in the device 1436 in a disabled form, and the root certifying authority 1402 enables the key 1408 in the device upon receipt and verification of the signed rules 1430")*

10. **As per dependent claim 19, 75 and 81 Sudia** discloses a method of enforcing a security policy in a cryptographic system, said policy including controlling use of a public key as applied to claims above. **Furthermore Sudia** d**iscloses a method wherein each user of the system has a private key,**[figure 14, ref. Num "1438", see private key] **and wherein said rules include:**

a rule requiring payment to a third party upon each use of said public key; [paragraph 0097] **a rule requiring payment to a third party upon each use of a user's private key**:[paragraph 0098]

a rule requiring payment to a third party upon each certification of a certificate's status; [paragraph 0102] or

a rule requiring payment to a third party upon each confirm-to transaction by a user[paragraph 0100]

11. **As per dependent claims 20, 76 and 82 Sudia** discloses a method of enforcing a security policy in a cryptographic system, said policy including controlling use of a public key as applied to claims above. **Furthermore Sudia** d**iscloses a method wherein**, said rules include a rule to pay for use by said recipient of intellectual property provided through the system.*[Paragraph 0110-0111, "see intellectual property licensing")*

12. **As per dependent claims 21,77 and 83 Sudia** discloses a method of enforcing a security policy in a cryptographic system, said policy including controlling use of a public key as applied to claims above. **Furthermore Sudia** d**iscloses a method wherein**, said user transaction is invalid until said digital signing is performed.[paragraph 0087-0088 & 0099, last sentence]

13. **As per dependent claims 72, 78 and 84 Sudia** discloses a method of enforcing a security policy in a cryptographic system, said policy including controlling use of a public key as applied to claims above. **Furthermore Sudia** d**iscloses a method** further comprising:

in response to said signing by said recipient, said certifying authority accepting a transaction from said recipient, said transaction based on said user transaction.[paragraph 0087-0088].

14. **As per dependent claims 80, Sudia discloses a method of enforcing a security policy in a crypto**graphic system, said policy including controlling use of a public key as applied to claims above. Furthermore Sudia discloses a method wherein said public key is a public key of a certifying authority, said providing is performed by a certifying authority, said digitally signing comprises hashing said message to obtain a hashed document, digitally signing said hashed document to form a digital agreement, and returning said digital agreement to said certifying authority, and said activating is performed by said certifying authority.[paragraph 0092-0094]

15. **As per dependent claims 109 and 128 Sudia discloses a method of enforcing a security policy in a crypto**graphic system, said policy including controlling use of a public key as applied to claims above. Furthermore Sudia discloses a method wherein **in a cryptographic system** *[See figure 14 and paragraph 0084, "cryptographic system"]* **wherein a certifying authority issues digital certificates identifying users of said system,***[paragraph 0085, figure 14, ref. Num "1404"] (on paragraph 0085, referring to figure 14, the following has been disclosed. "a certifying authority CA 1402 issues user identity certificate 1404 to users")* **said digital certificates being digitally signed with a private key of said certifying authority to form a digital signature [Paragraph 0085, figure 14, ref. Num "1410"]** *(On paragraph 0085, the following has been disclosed. "Certifying authority 1402 has a private key 1406 and a public key 1408. The private key 1406 is used to digitally sign the certificates 1404 with certifying authorities digital signatures 1401]* **and requiring a public key of said certifying authority in order to verify said digital signature, [paragraph 0086, last sentence]** *(On paragraph 0086, last sentence the following has been disclosed. "in order for the information contained in the certificates 1404 to be verified by other users of the system, these other users must have access to the public key 1408 of the certifying authority 1402)* **and wherein a**

participant transaction in said cryptographic system requires verification by a recipient of said user transaction, said verification based on information in said digital certificates and requiring said public key,[See paragraph 0086, last sentence, paragraph 0087 and paragraph 0091] *(On paragraph 0091, the following has been disclosed. "As noted above in order for the information contained in the various certificates to be verified by users of the system, these users must have access to the public key 1408 of the certifying authority 1402")* **the verification is based on information in a digital certificate and requiring public key.***[paragraph 0087-0088]*

16. **As per dependent claims 110, 115-116, 120, 125 and 130 Sudia discloses a method of enforcing a security policy in a crypto**graphic system, said policy including controlling use of a public key as applied to claims above. Furthermore Sudia discloses a method wherein *the public key in the secure device becomes inactive after a certain time period, the method further comprising: after the public key becomes inactive, in response to a demonstration by the recipient of agreement or consistency with one or more of the rules, activating the inactive public key in the secure device.[paragraph 0095]*

17. **As per dependent claims 111, 113,117,121,126,129 and 131 Sudia discloses a method of enforcing a security policy in a crypto**graphic system, said policy including controlling use of a public key as applied to claims above. Furthermore Sudia discloses a method, wherein said demonstration includes information from the secure device identifying operational capabilities of the secure device and further including information uniquely binding said recipient to said demonstration by the recipient of agreement or consistency with one or more of the rules.*[paragraph 0095-0096]*

18. **As per dependent claims 112 and 118 Sudia discloses a method of enforcing a security policy in a crypto**graphic system, said policy including controlling use of a public

key as applied to claims above. Furthermore Sudia discloses a method, wherein the public key is certified by an authority.[0084-0086]

19. **As per dependent claim 114, Sudia discloses a method of enforcing a security policy in a crypto**graphic system, said policy including controlling use of a public key as applied to claims above. Furthermore Sudia discloses a method, wherein the rules comprise a rule regarding maintaining secrecy of the public key.[paragraph 0092]

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W. Dada whose telephone number is (571) 272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.
Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

07/01/2008

/Beemnet W Dada/

Examiner, Art Unit 2135

/KimYen Vu/

Supervisory Patent Examiner, Art Unit 2135